UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

UNITED STATES OF AMERICA, Plaintiff, v. MURUGANANANDAM ARUMUGAM, Defendant.	Case No. 19-CR-41-RSL ORDER DENYING DEFENDANT'S MOTION TO COMPEL DISCOVERY

This matter comes before the Court on defendant's "Motion to Compel Production of Discovery." Dkt. #67. Defendant moves for production of certain discovery in relation to his motion to suppress (Dkt. #43), which is scheduled for oral argument on March 3, 2020.[1] For the reasons set forth below, defendant's motion to compel is DENIED.[2]

I. BACKGROUND

Defendant Murugananandam Arumugam is charged with one count of possession of child pornography in violation of 18 U.S.C. §§ 2252(a)(4)(B), (b)(2), and one count of receipt of child pornography in violation of 18 U.S.C. §§ 2252(a)(2), (b)(1). See Dkt. #84 (Second Superseding Indictment).

[1] Defendant also has a second, related motion to suppress pending for hearing before the Court. See Dkt. #44.

[2] The Court, having reviewed the memoranda, declarations, and exhibits submitted by the parties, finds that resolution of this matter without oral argument is appropriate.

On October 1, 2019, defendant filed a motion to suppress[3] all evidence and fruits of that evidence seized as a result of the government's use of the RoundUp eMule ("RoundUp") program to investigate defendant's activity on a peer-to-peer (P2P) file sharing network. See Dkt. #43; Dkt. #71-1 (Lynn Decl.) at ¶ 3. RoundUp is a modified version of the public eMule P2P client used to conduct undercover child pornography investigations. Lynn Decl. at ¶ 21.[4] The government's implementation of RoundUp led to Detective Daniel Conine downloading from IP address 73.11.164.229 files and partial files of minors engaging in sexually explicit conduct. Accordingly, RoundUp was the means through which law enforcement identified defendant as a suspect and established the bases for two search warrants: (1) to obtain IP address subscriber information from Comcast, and (2) to search and seize computers and electronic storage devices from defendant's residence in Redmond, Washington. See Dkt. #44-1 at 18-21. During the search of defendant's home, agents seized several items, including a Dell computer containing visual depictions of minors engaged in sexually explicit conduct. The charges pertain to the items seized during the search of defendant's home.

Defendant's motion to suppress advances two legal theories to support his contention that the government's use of RoundUp constituted an unlawful "search" on defendant's computer in violation of the Fourth Amendment. Defendant argues that "[a] warrantless search occurred because" (1) "the government identified IP address 73.11.164.229, port 54494 after it engaged in generalized surveillance using technology unavailable to the public"; and (2) "the government digitally trespassed into the device connected to IP address 73.11.164.229, port 54494 after it engaged in generalized surveillance using technology unavailable to the public." See Dkt. #67 at 2.

[3] The motions to suppress were re-noted for the Court's consideration on February 14, 2020. See Dkt. #69.

[4] The government's expert, Bryan Lynn, identifies four modifications that differentiate RoundUp from eMule: (1) preventing of file sharing on the eMule network, (2) downloading of files from a single source rather than from multiple eMule clients, (3) documenting the single source download activity, and (4) the ability to search the network specifically for files suspected of being associated with child pornography. Lynn Decl. at ¶ 22.

The government filed its response to defendant's motion to suppress on November 15, 2019. See Dkt. #60. On November 25, 2019, defendant served the government with a Federal Rule of Criminal Procedure ("Rule") 16(a)(1)(E) discovery request related to the government's arguments in response to his motion to suppress. See Dkt. #67-1, 67-2 (Ex. A). Defendant raised 13 categories of evidence, asserting their materiality to his preparation for the pre-trial motion to suppress litigation. Dkt. #67 at 2; Dkt. #67. Defendant's letter specifically requested:

1) A copy of the RoundUp eMule User Manual for version 1.57
2) A copy of the RoundUp eMule source code for version 1.57
3) A copy of all test specifications, procedures, protocols, and test results used to test RoundUp eMule
4) How many hash values are stored in the list of previously identified hash values?
5) How many of the hash values stored in the previously identified hash values are known child pornography?
6) How many of the hash values stored in previously identified hash values are alleged child pornography?
7) How many of the hash values stored in the previously identified hash values are related to child pornography but not known or alleged?
8) All records and fields from the download candidate database for the IP address involved in this case, IP address: 73.11.164.229. Production in an Excel spreadsheet format is preferred.
9) Identify all records in the download candidate database for IP address: 73.11.164.229 that were logged by RoundUp eMule computers operating outside the U.S.
10) The total number of computers running RoundUp eMule and logging search results in the download candidate database during the entire period of time that IP address 73.11.164.229 was being surveyed. This would be the period of time from the logging of the first search result for IP address 73.11.164.229 until the last search result stored for that IP address. The total number is for all computers logging search results for all IP addresses.
11) Total number of RoundUp eMule computers from request 10) that were operating outside the U.S. Courts

12) The name of a currently available software program that executes automated Google searches and aggregates the results

13) All RoundUp and eMule log files from Det. Conine's computer. The log files originally produced only extend through 4/17/2017. According to the clients.met file on Mr. Arumugam's computer Det. Conine's computer had downloaded data on 10/2/2017. Provide the missing RoundUp eMule log files from 4/17/2017.

Dkt. #67-2 (Ex. A). According to defendant, defense attorneys met with the government to discuss the discovery demand on December 4, 2019, when the government indicated it would not agree to the request. Dkt. #67 at 3. On December 18, 2019, the government served the defense with a letter opposing defendant's 13 discovery requests. See Dkt. #67-3 (Ex. B). On December 31, 2019, defendant filed the instant motion to compel the government's production of the 13 discovery items identified in his November 25, 2019 discovery demand. See Dkt. #67.

II. DISCUSSION

In relevant part, Rule 16(a)(1)(E) provides,

> Upon a defendant's request, the government must permit the defendant to inspect and to copy or photograph books, papers, documents, data, photographs, tangible objects, buildings or places, or copies or portions of any of these items, if the item is within the government's possession, custody, or control and . . . the item is material to preparing the defense.

Fed. R. Crim. P. 16(a)(1)(E). The disclosure requirement is not necessarily limited to preparation for trial defense. See United States v. Soto-Zuniga, 837 F.3d 992 (9th Cir. 2016) (concluding that "Rule 16(a)(1)(E) permits discovery to determine whether evidence in a particular case was obtained in violation of the Constitution and was thus admissible"). In support of his motion, defendant argues that (1) the requested items are in the government's possession, custody, or control; (2) the requested items are material to the pre-trial litigation; and (3) any concerns underlying the government's claim of qualified law enforcement privilege can be resolved with a protective order. See Dkt. #67.

a. Government's Possession, Custody, or Control

The first issue is whether the items defendant requests are in the government's possession, custody, or control. See Fed. R. Crim. P. 16(a)(1)(E). Defendant argues that the RoundUp source code, user manual, and all related items identified in Exhibit A are in the government's possession, custody, or control because the government's expert has access to the information and receives funding from the U.S. Department of Justice to develop and manage RoundUp. See Dkt. #67 at 4-5.[5] The Court declines to reach the question of government possession, because even assuming defendant's requested items are in the possession, custody, or control of the government, defendant fails to establish the materiality of the requested evidence for the reasons set forth below.

b. Materiality

"A defendant must make a 'threshold showing of materiality' in order to compel discovery pursuant to Rule 16(a)(1)(E)." United States v. Budziak, 697 F.3d 1105, 1111 (9th Cir. 2012) (citation omitted). "Neither a general description of the information sought nor conclusory allegations of materiality will suffice; a defendant must present facts that would tend to show that the [g]overnment is in possession of information helpful to the defense." Id. at 1111-12 (citation omitted).

Defendant argues that the requested discovery is material to the two Fourth Amendment theories in his motion to suppress, as outlined above. See Dkt. #67 at 5-7. He argues that the requested items, including the RoundUp source code and user manual, are necessary to show that RoundUp used "tagging" or "tracing" methods that resulted in an unlawful search. He also argues that he will not be able to effectively cross-examine the government's expert on the search issue, or develop an adequate factual record with all of the information the government possesses. Defendant asserts that his requests are necessary because "the government's expert is in disagreement with the defense expert on the question of whether there was a search of

[5] The government's expert, Bryan Lynn, is the developer of RoundUp. See Dkt. #71-1 (Lynn Decl.). The government also relies on expert Detective Robert Erdely with the Indiana County Pennsylvania Computer Crime Unit, who assisted in developing RoundUp and is a subject matter expert on P2P networks. See Dkt. #71-2 (Erdely Decl.).

[defendant's computer]." Dkt. #67 at 5-6. Defendant seeks the RoundUp source code, user manual, test results, and related evidence so that his own expert, Terry Lahman, may perform his own tests on the program, which defendant believes will prove the existence of a government search.[6] See Dkt. #67 at 6-7; Dkt. 75

In support of his argument for an order compelling production of the RoundUp source code, user manual, and technical specifications, defendant relies on United States v. Budziak, 697 F.3d 1105 (9th Cir. 2012). Although binding upon this Court, Budziak is distinguishable.[7] Budziak involved a defendant's motion to compel disclosure of the source code and technical specifications of EP2P, another P2P program similar to an enhanced version of LimeWire. Id. at 1112-13. The defendant in Budziak argued that the FBI, using EP2P, only downloaded certain fragments of child pornography files from his computer, which he alleged raised doubts about whether he knowingly distributed complete child pornography files and whether the law enforcement officials might have used the program to override defendant's sharing settings on LimeWire. Id. at 1112. If true, the defendant argued, the requested discovery would tend to negate the mens rea element of the charged crime, a central element to his defense. Id.

[6] Of note, the government offered to provide a demonstration of RoundUp to defendant's counsel and expert, in which Detective Erdely or Detective Conine could "(1) [describe] how investigators use RoundUp eMule to identify and download child pornography from P2P network users; (2) describe its manual and automated search and download capabilities; and (3) demonstrate several single source downloads, explaining how those downloads are logged and how to interpret the log files produced by RoundUp eMule." See Dkt. #71 at 8; Dkt. #67-3 (Ex. B) at 2. The government indicates that defendant declined this offer and instead filed the instant motion to compel. Dkt. #71 at 8.

[7] Neither is defendant's reliance on United States v. Soto-Zuniga, 837 F.3d 992 (9th Cir 2016) persuasive. See Dkt. #75 at 5. The defendant in Soto-Zuniga challenged the district court's denial of his motion to compel discovery of a Border Patrol checkpoint's arrest and search statistics. Id. at 995. The Ninth Circuit found the district court abused its discretion in denying the motion to compel, concluding that defendant had made a specific showing as to how those arrest and search statistics were "material" to his defense that the border checkpoint violated his Fourth Amendment rights. Id. at 999-1002. As the Court in Blouin emphasized, "[s]earch and arrest statistics are substantially different from source code." Blouin, 2017 WL 2573993, at *3 n.3 (citing Soto-Zuniga, 837 F.3d at 999-1002). Further, defendant's conclusory assertions as to the possibility that the RoundUp source code and technological specifications would assist him in supporting his Fourth Amendment challenge fall short of the requisite showing under Rule 16(a)(1)(E).

Defendant has not made any similar showing here.[8] While defendant argues that he needs access to the RoundUp source code and technical specifications in order to "assess the program and testimony of FBI agents who used it to build the case against him," Dkt. #67 at 5-6 (quoting Budziak, 697 F.3d at 1112), and to allow his expert to prove the existence of a government search, he offers only a declaration from his expert and his expert's letter listing discovery requests to support his conclusory speculations. See Dkt. #43 (Ex. B); Dkt. #67-2 (Ex. A). Defendant has failed to demonstrate with specificity how the information he seeks is material to any defense, especially considering that he, unlike the defendant in Budziak, has not been charged with any of the conduct Detective Conine observed on RoundUp. See Dkt. #71 at 21; Dkt. #84.

The Court also agrees with the government that defendant has failed to show how the additional hash values and information regarding the government's download candidate database are relevant to his case. See Dkt. #71 at 22-23. Defendant does not dispute the government's assertion that he has access to the nearly 3,000 hash values associated with the child pornography files actually involved with this case. Id. at 9, Ex. B (Erdely Decl) at ¶ 5, 18; Ex. A (Lynn Decl.) at ¶ 20; see also Dkt. #67, 75. Defendant fails to support his request for broader discovery related to hash values or the download candidate database, which largely concern other individuals suspected of sharing child pornography. Dkt. #71-2 (Erdely Decl.) at ¶¶ 6-7, 18. Accordingly, defendant has not established materiality with regard to his requests for additional hash values or law enforcement's download candidate database.

c. Qualified Law Enforcement Privilege

Finally, the Court shares the government's concerns regarding the sensitivity of RoundUp, its source code, hash value and download candidate databases, and related evidence. Dkt. #71 at 23-27; see also Blouin, 2017 WL 2573993, at *3 (quoting United States v. Pirosko, 787 F.3d 358, 365 (6th Cir. 2015)) (agreeing that "granting the defendant's request for the

[8] The Court also notes that numerous decisions, including one within this District, have since distinguished Budziak on similar grounds. See, e.g., United States v. Blouin, No. CR16-307 TSZ, 2017 WL 2573993, at *3 (W.D. Wash. June 14, 2017); United States v. Feldman, 2014 WL 7653617, at *5-6 (E.D. Wis. July 7, 2014).

[RoundUp] source code would 'compromise the integrity of [the government's] surveillance system and would frustrate future surveillance efforts"). However, because defendant has not met his burden to establish the materiality of the requested evidence, the Court declines to reach the merits of the government's law enforcement privilege argument.[9]

III. CONCLUSION

For all the foregoing reasons, defendant's Motion to Compel Production of Discovery (Dkt. #67) is DENIED.

DATED this 27th day of February, 2020.

Robert S. Lasnik
United States District Judge

[9] Similarly, the Court need not reach defendant's arguments on reply regarding his due process and Confrontation Clause rights. See Dkt. #75 at 8-9. Because defendant has not established that the requested information is material to his defense, he fails to show that his constitutional rights will be violated by the Court's denial of his motion to compel.